УДК 004.056

Можаєв Олександр Олександрович, д-р техн. наук, кафедра мультимедійних технологій та систем. Національний технічний університет «Харківський політехнічний інститут», *м Харків, Україна. вул. Фрунзе, 21, м. Харків, Україна, 61024. Тел. , E-mail: mozhaev57@mail.ru, (orcid.org/ 0000-0002-1412-2696)*
Семенов Сергій Геннадійович, д-р техн. наук, кафедра обчислювальної техніки та програмування. Національний технічний університет «Харківський політехнічний інститут» *м Харків, Україна. вул. Фрунзе, 21, м. Харків, Україна, 61024. Тел. , E-mail: (orcid.org/)*
Можаєв Михайло Олександрович, аспірант, Національний технічний університет «Харківський політехнічний інститут» *E-mail: mozhayev_misha@inbox.ru (orcid.org/ 0000-0003-1566-9260)*
Казімірова Віра Василівна, викладач-стажист. Національний технічний університет «Харківський політехнічний інститут» *E-mail: werakazimirova@gmail.com (orcid.org/ 0000-0003-1337-6421)*
Кузьменко Вікторія Євгенівна, аспірант, Національний технічний університет «Харківський політехнічний інститут», *E-mail: (orcid.org/)*

ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ ЗАХИСТУ ДАНИХ В ІНФОРМАЦІЙНІЙ УПРАВЛЯЮЧІЙ СИСТЕМІ КРИТИЧНОГО ЗАСТОСУВАННЯ

У статті проведена оцінка ефективності методів і способів розподілу доступу та захисту даних а також представлені методичні рекомендації щодо їх використанні в комп'ютеризованих інформаційних управляючих системах (КІУС) критичного застосування. Розроблено імітаційну модель системи розподілу доступу та захисту інформації в КІУС критичного застосування.

Ключові слова: *комп'ютеризовані інформаційні управляючі системи критичного застосування, зовнішні зловмисні дії, розподіл доступу, захист інформації.*

Можаев Александр Александрович, д-р техн. наук, кафедра мультимедийных технологий и систем. Национальный технический университет «Харьковский политехнический институт», г. Харьков, Украина. *ул. Фрунзе, 21, м. Харьков, Украина, 61024. Тел. , E-mail: mozhaev57@mail.ru*, (*orcid.org/ 0000-0002-1412-2696)*
Семенов Сергей Геннадиевич, д-р техн. наук, кафедра вычислительной техники и программирования. Национальный технический университет «Харьковский политехнический институт» г. Харьков, Украина. *ул. Фрунзе, 21, м. Харьков, Украина, 61024. Тел. , E-mail: (orcid.org/)*
Можаев Михаил Александрович, аспирант, Национальный технический университет «Харьковский политехнический институт» *E-mail: mozhayev_misha@inbox.ru (orcid.org/ 0000-0003-1566-9260)*
Казимирова Вера Васильевна, преподаватель-стажер. Национальный технический университет «Харьковский политехнический институт» E-mail: *werakazimirova@gmail.com (orcid.org/ 0000-0003-1337-6421)*
Кузьменко Виктория Евгеньевна, аспирант, Национальный технический университет «Харьковский политехнический институт» *E-mail: (orcid.org/)*

ОЦЕНКА ЭФФЕКТИВНОСТИ МЕТОДОВ ЗАЩИТЫ ДАННЫХ В ИНФОРМАЦИОННЫХ УПРАВЛЯЮЩИХ СИСТЕМАХ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

В статье проведена оценка эффективности методов и способов распределения доступа и защиты данных а также представлены методические рекомендации по их использовании в компьютеризированных информационных управляющих системах (КИУС) критического применения. Разработана имитационная модель системы распределения доступа и защиты информации в КИУС критического применения.

Ключевые слова: *компьютеризированные информационные управляющие системы критического применения, внешние злонамеренные действия, распределение доступа, защита информации.*

Mozhayev Olexander,. D. Sci, Kharkiv National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine. *Str. Frunze, 21, Kharkov, Ukraine, 61024. Tel.. E-mail: mozhaev57@mail.ru, (orcid.org/* 0000-0002-1412-2696*)*
Semenov Sergei Genadievich, D. Sci, Kharkiv National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine. *Str. Frunze, 21, Kharkov, Ukraine, 61024. Tel. .E-mail: (orcid.org/)*
Mozhaiev Mykhailo, aspirant, National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine. E-mail: mozhayev_misha@inbox.ru (orcid.org/0000-0003-1566-9260)
Kazimirova Vera, teacher trainee, National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine. *E-mail: werakazimirova@gmail.com (orcid.org/ 0000-0003-1337-6421)*
Kuzmenko Viktoria Evgenievna, aspirant, National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine. *E-mail: (orcid.org :)*

ASSESS THE EFFECTIVENESS OF METHODS IN A INFORMATION MANAGEMENT SYSTEM CRITICAL APPLICATIONS

The paper assessed the effectiveness of methods and ways of distribution of access and data protection as well as provides guidelines for their use in computerized information management systems (KIUS) critical applications. A simulation model of the distribution system of access and protection of information in KIUS critical applications.

Keywords: *computerized information and control systems of critical applications, external malicious activities, the distribution of access, information security*

Введение

Одним из наиболее важных этапов разработки методов и средств распределения доступа и защиты данных в КИУС критического применения является имитационное моделирование и экспериментальное исследование [2–7]. При этом их целью должно быть решение таких частных задач:

– проверка адекватности разработанных моделей и методов распределения доступа и защиты данных в КИУС критического применения;

– анализ достоверности полученных результатов в ходе решения оптимизационных задач настройки параметров распределения доступа в КИУС критического применения;

– обоснованный выбор показателей и оценка по ним эффективности разработанных моделей и методов;

– разработка научно-практических рекомендаций по их использованию в современных и перспективных КИУС критического применения.

Анализ литературы [1–7] показал, что в ходе решения этих задач на основании проведенных исследований и опыте практической эксплуатации КИУС критического применения необходимо принимать решения о способах возможного использования аналитического и имитационного моделирования, а также возможного лабораторного эксперимента. Традиционно с помощью математического моделирования можно получить при различных исходных данных достаточно широкий спектр результатов, требующих уточнения в ходе имитационного моделирования и эксперимента. То есть, средства математического моделирования должны органично дополняться возможностями имитационной модели и лабораторной базы.

Оценка эффективности методов и средств защиты данных в КИУС критического применения

Для обоснования достоверности полученных результатов и оценки эффективности методов распределения доступа и защиты данных в КИУС критического применения было проведено имитационное моделирование систем идентификации состояния и адаптивного управления безопасностью в КИУС критического применения. В качестве инструментария имитационного моделирования используем среду символьной математики MathCAD-14, специализированные программы формирования квазициклов и вычисления BDS-статистики, сбора параметрической информации КИУС критического применения и принятия решения о состоянии системы [3].

Обобщенная структурная схема разработанной имитационной модели систем идентификации состояния и адаптивного управления безопасностью в КИУС критического применения приведена на рис. 1.

Сбор исходной информации о состоянии КИУС критического применения (загрузка центрального процессора – x_1, оперативной памяти – x_2 и сетевого устройства – x_3) осуществлялся с помощью специально разработанного программного комплекса и стандартного программного анализатора трафика (например, «Wireshark»).

Структура программного комплекса сбора входной информации приведена на рис. 2.

Как видно из рис. 2 в состав программного комплекса входят же модули: сенсоры сетевой активности, загрузка центрального процессора (ЦП) и оперативной памяти (ОП), реализация математического аппарата обработки статистических данных, служебная часть.

Каждый модуль программного комплекса решает отдельный класс реализуемых задач, а именно:

Сенсор сетевой активности (реализован на базе стандартного программного анализатора трафика): захват и фильтрация передаваемого через наблюдаемый сетевой интерфейс трафика,

накопления статистической информации в заданных параметрах наблюдения и дальнейшее преобразование к единому виду представления статистической выборки, передача статистических данных на обработку в модуль обработки данных и формирования наблюдаемого структурно-информационного портрета.

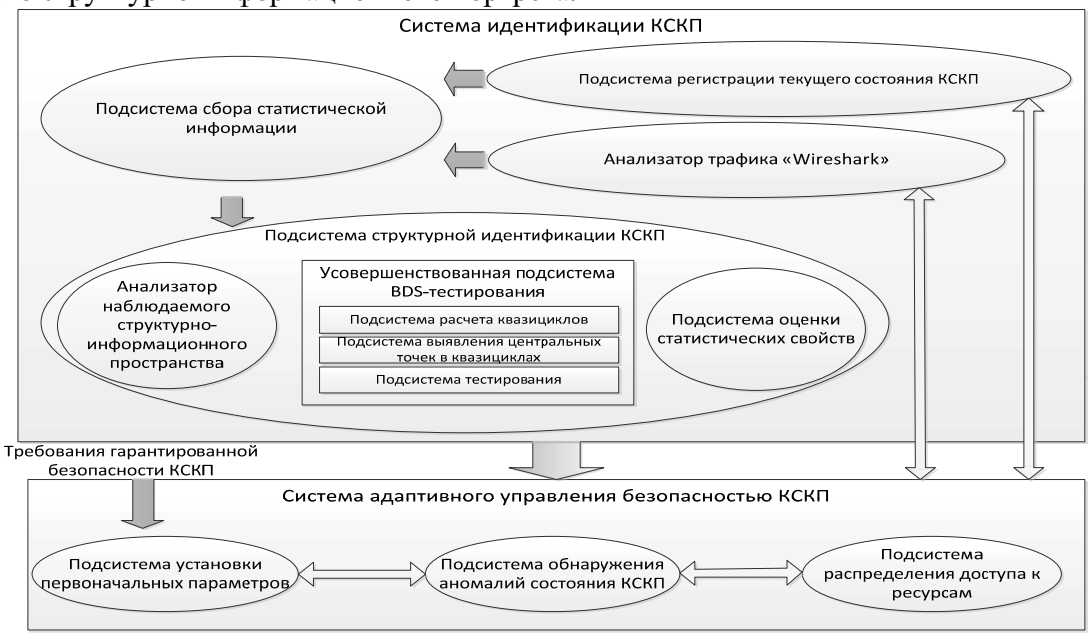


Рис. 1. Обобщенная структурная схема разработанной имитационной модели систем идентификации и адаптивного управления безопасностью КИУС критического применения

Рис. 2. Структура программного комплекса сбора входной информации

Модуль обработки данных и формирования наблюдаемого структурно-информационного портрета: отдельное хранение статистических данных об интервалах наблюдений, соответствующих предыдущих этапов наблюдения для каждого вида наблюдений загрузки статистических данных о предыдущих аналогичные интервалы при изменении интервала наблюдения, загрузки статистических данных в режиме реального времени, формирования наблюдаемых структурно-информационных портретов КИУС критического применения.

Как видно из рис. 2 основными элементами сбора статистической информации есть соответствующие сенсоры. Во сенсором понимается программное средство, предназначенное для получения информации об одной или нескольких характеристиках элементов.

При моделировании сенсоров загрузки ЦП и оперативной памяти были использованы стандартные процедуры GetSystemTimes [8], заложенные в библиотеку Win 32. Диаграмма последовательностей действий сбора статистических данных и диаграмма классов в программе

приведена на рис. 3 и рис. 4 соответственно.

Внешний вид интерфейса указанной подсистемы приведена на рис. 5. Количество и характер трафика, поступающего в КИУС критического применения, различные варианты внешних воздействий задавались с помощью программного пакета IxChariot и лабораторной установки моделирования.

Структура лабораторной установки приведена на рис. 6.

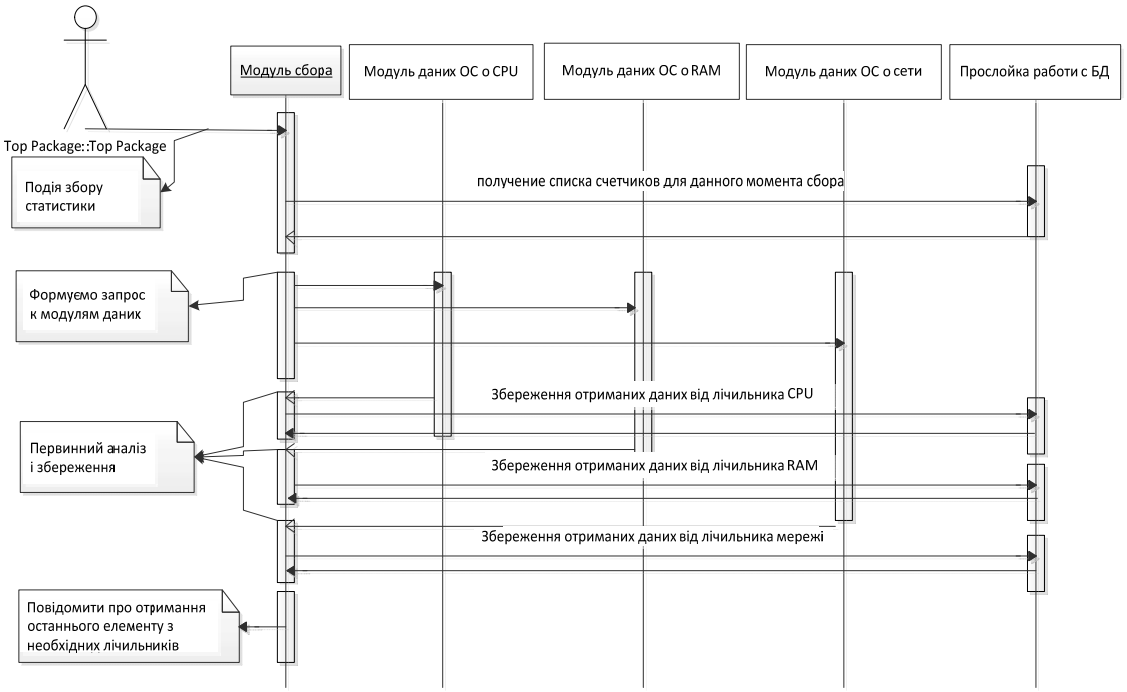


Рис. 3. Диаграмма последовательностей действий сбора статистических данных

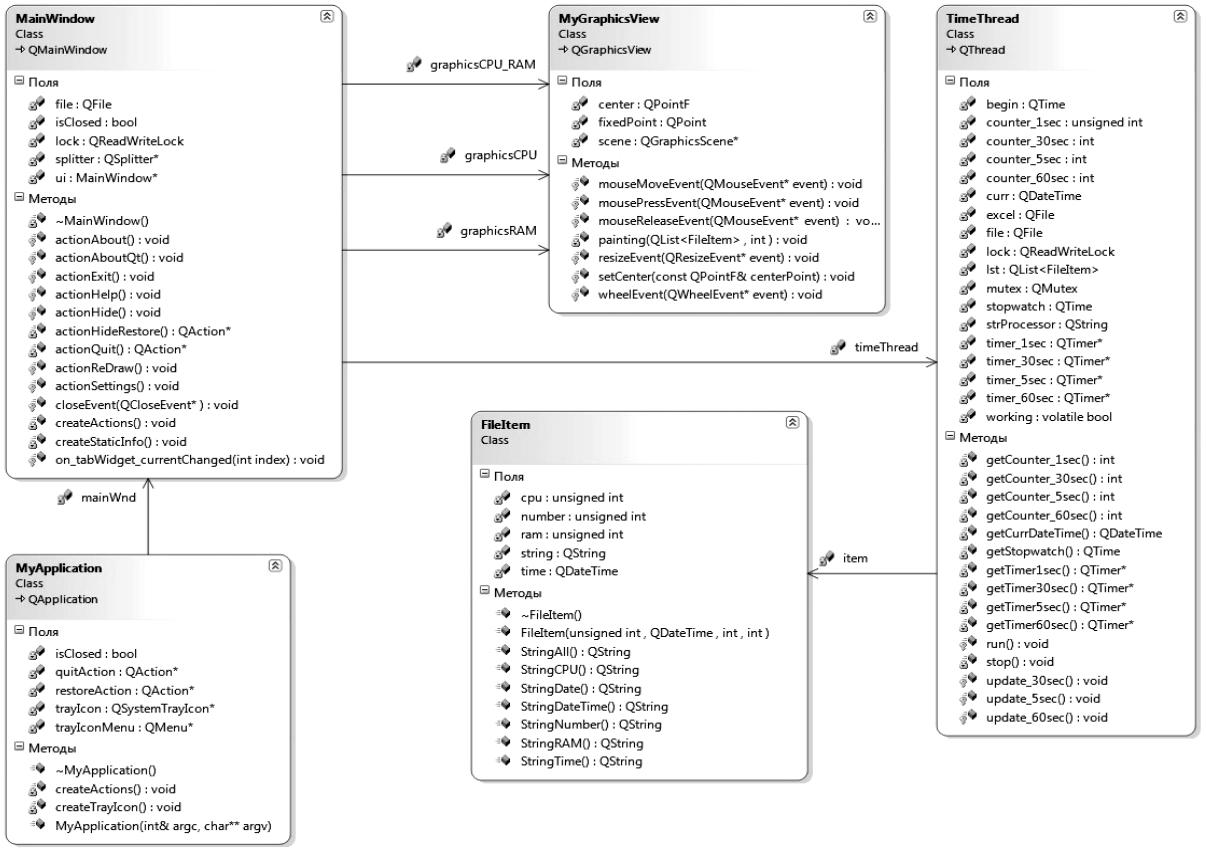
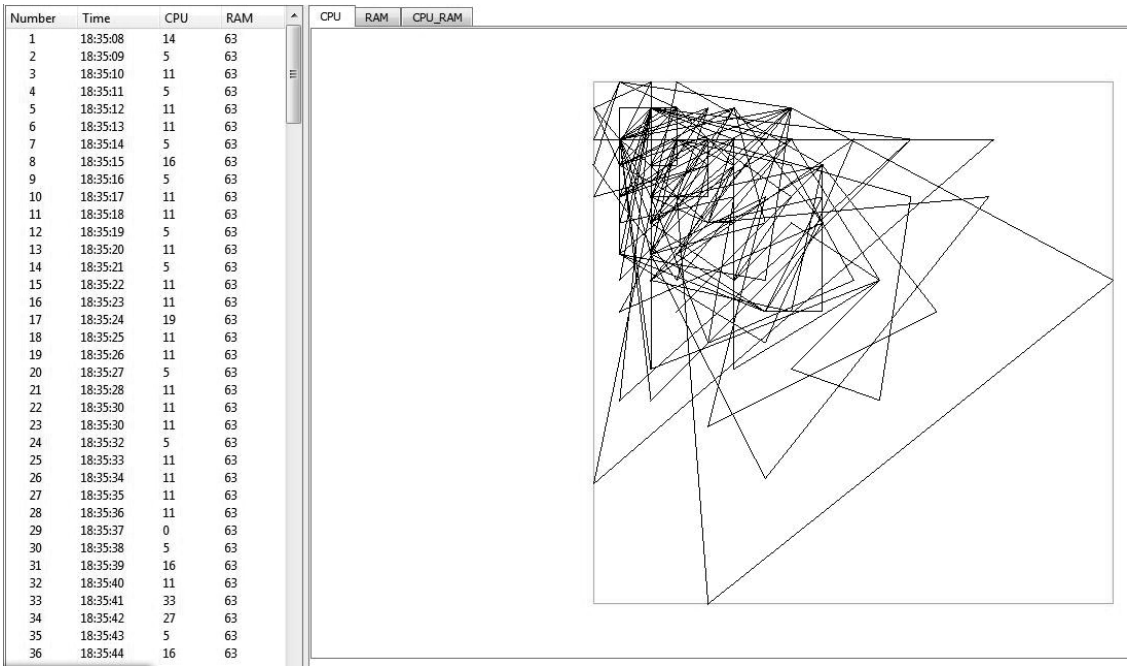


Рис. 4. Диаграмма классов в программе



Number	Time	CPU	RAM
1	18:35:08	14	63
2	18:35:09	5	63
3	18:35:10	11	63
4	18:35:11	5	63
5	18:35:12	11	63
6	18:35:13	11	63
7	18:35:14	5	63
8	18:35:15	16	63
9	18:35:16	5	63
10	18:35:17	11	63
11	18:35:18	11	63
12	18:35:19	5	63
13	18:35:20	11	63
14	18:35:21	5	63
15	18:35:22	11	63
16	18:35:23	11	63
17	18:35:24	19	63
18	18:35:25	11	63
19	18:35:26	11	63
20	18:35:27	5	63
21	18:35:28	11	63
22	18:35:30	11	63
23	18:35:30	11	63
24	18:35:32	5	63
25	18:35:33	11	63
26	18:35:34	11	63
27	18:35:35	11	63
28	18:35:36	11	63
29	18:35:37	0	63
30	18:35:38	5	63
31	18:35:39	16	63
32	18:35:40	11	63
33	18:35:41	33	63
34	18:35:42	27	63
35	18:35:43	5	63
36	18:35:44	16	63

Рис. 5. Интерфейс программной системы сбора статистических данных о состоянии КИУС критического применения

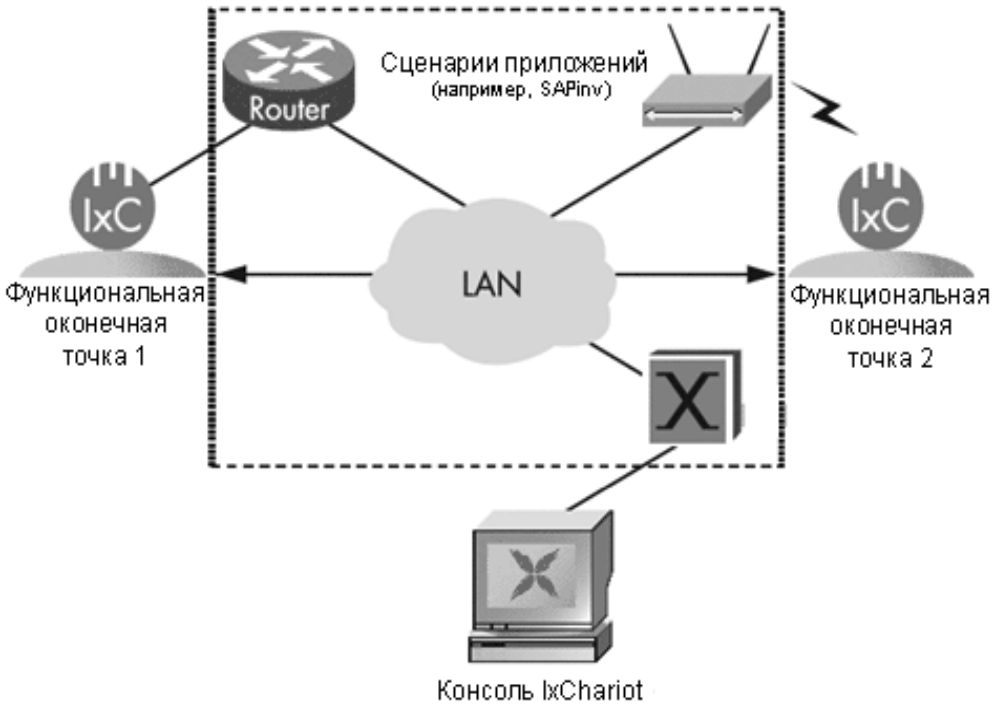


Рис. 6. Структура лабораторной установки моделирования

Проведенные исследования показали, что в разработанной имитационной модели основой подсистемы структурной идентификации состояния КИУС критического применения является анализатор наблюдаемого структурно-информационного пространства, усовершенствованная подсистема BDS-тестирования и подсистема оценки статистических свойств.

Входными данными для указанных подсистем является в первую очередь вероятностно-временные характеристики, определяющие состояние системы (множество X), также

статистические данные о поведении информационного потока различных телекоммуникационных служб [2–7].

Функционирование всех приведенных подсистем имеет целью реализацию принципа оптимального распределения информационных ресурсов с учетом текущего состояния КИУС критического применения и требований гарантированной безопасности к ним.

Таким образом, разработанная имитационная модель систем идентификации состояния и адаптивного управления безопасностью КИУС критического применения осуществляет сбор и статистическую оценку данных о состоянии КИУС критического применения, а также входного информационного потока, идентифицирует состояние КИУС критического применения, обнаруживает аномалии в ее поведении и осуществляет перераспределение доступа к ресурсов КИУС критического применения исходя из данных о состоянии системы. Результаты имитационного моделирования позволят оценить эффективность методов и средств распределения доступа и защиты данных в КИУС критического применения.

Используя методы и приемы математического и имитационного моделирования оценим эффективность разработанных моделей и методов распределения доступа и защиты данных в КИУС критического применения, проведем сравнительные исследования с известными методами [2–7].

Для подтверждения эффективности разработанного метода по сравнению с методами, основанным на принципах ролевого и мандатной доступа, приведем графики (рис. 7) зависимости времени функционирования системы в безопасном режиме $T_б$ от отношения интенсивности злонамеренной атаки $I_{атаки}$ к интенсивности входного потока $I_{сд}$ санкционированных данных (на примере Dos-атаки – участок 4, MAC-flooding-атаки – участок 3, R2L-атаки – участок 2 и Probe-атаки – участок 1).

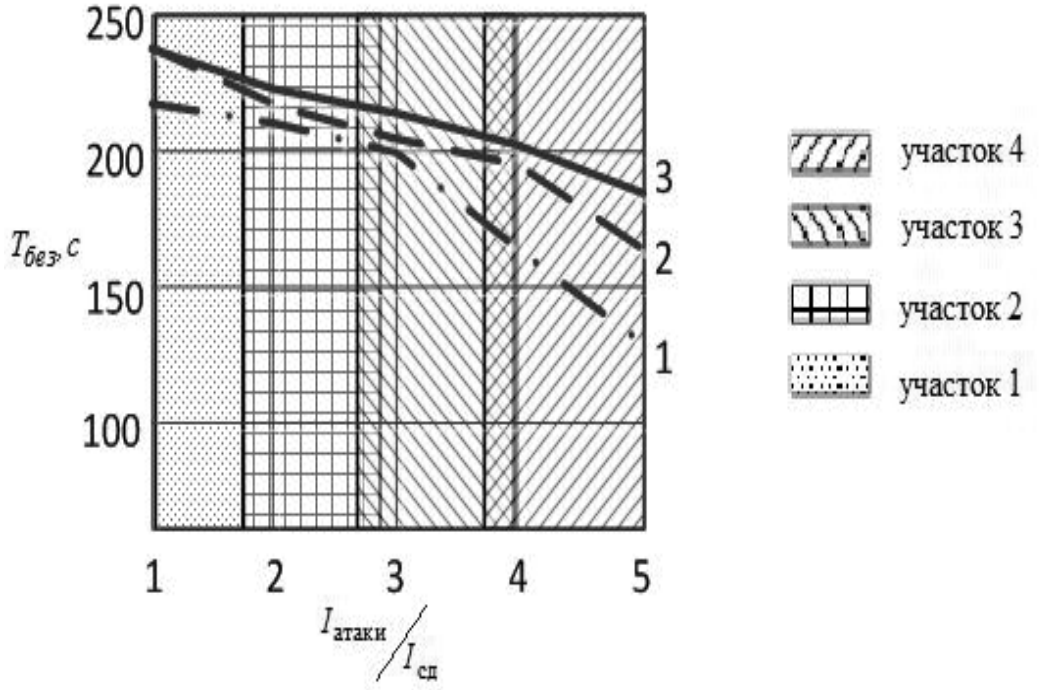


Рис. 7. Зависимость времени $T_{без}$ от отношения интенсивностей $I_{атаки}/I_{сд}$

На графике рис. 7 приведено семейство кривых зависимости $T_б$ от $I_{атаки}/I_{сд}$ в условиях использования разработанных методов и средств распределения доступа и защиты данных (кривая 3), метода мандатного распределения доступа (кривая 2) и метода ролевого распределения доступа (кривая 1).

Как видно в целом с рис. 7 существует четкая тенденция снижения уровня времени

функционирования системы в безопасном режиме при увеличении интенсивности атаки. В то же время рис. 7 иллюстрирует преимущества разработанных методов и средств распределения доступа и защиты данных в КИУС критического применения по сравнению с методами ролевого и мандатной доступа. Особенно это заметно при высокой интенсивности вредоносных атак. Так использование разработанных методов и средств распределения доступа и защиты данных в КИУС критического применения позволяет выполнить требования гарантированного уровня безопасности в условиях, когда интенсивность $I_{атаки}$ превышает интенсивность санкционированного доступа $I_{сд}$ до 5 раз, в то же время когда другие методы (мандатной и ролевого доступа) могут обеспечить данные требования только при меньших значениях интенсивностей вредоносных воздействий.

В целом следует отметить, что использование разработанных методов позволит повысить уровень безопасности информации в 1,1 раза при низкой интенсивности внешних воздействий $\left(\frac{I_{атаки}}{I_{сд}} \le 1\right)$, и до 1,5 раза при высокой интенсивности воздействий $\left(\frac{I_{атаки}}{I_{сд}} > 1\right)$.

Таким образом, исследования показали целесообразность использования разработанных методов и средств распределения доступа и защиты данных в условиях внешних воздействий для обеспечения гарантированного уровня безопасности.

1. Рекомендации по практическому применению методов и средств распределения доступа и защиты данных в КИУС критического применения на этапе проектирования

Проведенные исследования показали, что при разработке архитектуры в процессе проектирования и особенно внедрение разработанных методов и средств распределения доступа и защиты данных следует использовать ряд рекомендаций, которые помогут избежать обычных проблем в каждой из исследованных областей защиты данных [1] :

- аутентификация;
- авторизация;
- управления конфигурацией;
- управления исключениями;
- протоколирование и инструментовки;
- управления состоянием.

Проектирование эффективной стратегии *аутентификации* имеет большое значение с точки зрения обеспечения безопасности и надежности программы, в противном случае, оно будет уязвимым для атак с подделкой пакетов, атак перебором по словарю, перехватом сеансов и других типов атак. При проектировании стратегии аутентификации необходимо руководствоваться следующими рекомендациями:

– Определите границы доверия и проводите аутентификацию пользователей и вызовов на границах доверия. Учтите, что может потребоваться аитентификуваты вызовы, как клиента, так и сервера (взаимная аутентификация).

– Обеспечьте использование надежных паролей или парольных фраз.

– При наличии множества систем в рамках программы, или если пользователи должны иметь возможность доступа ко многим приложений, используя одни и те же учетные данные, используйте стратегию единой регистрации.

– Не передавайте пароли по сети и не храните их в базе данных или хранилище данных в открытом виде. Храните хэш пароля.

Проектирование эффективной стратегии *авторизации* имеет большое значение с точки зрения обеспечения безопасности и надежности программы, в противном случае, оно будет уязвимым для разглашения сведений, повреждения или подделки данных и несанкционированного получения прав. При проектировании стратегии авторизации руководствуйтесь такими рекомендациями:

– Определите границы доверия и проводите авторизацию пользователей и вызовов на границах доверия.

– Защитите ресурсы, проводя авторизацию вызывающей стороны на основании ее удостоверения, групп или ролей. Обеспечьте минимальное дробления, по возможности ограничивая количество используемых ролей.

– Применяйте авторизацию на базе ресурсов для аудита системы. При авторизации на базе ресурсов права доступа определяются в самом ресурсе. Например, список управления доступом (ACL) ресурса Windows использует удостоверение исходного вызывающего для определения его прав доступа к ресурсу. При использовании авторизации на базе ресурсов в WCF необходимо выполнить олицетворение исходного вызывающего через клиента или слой представления, через слой сервисов WCF и для кода бизнес-логики, выполняет доступ к ресурсу.

– Используйте авторизацию на основании утверждений, если нужно поддерживать интегрированную авторизацию на базе сочетания данных, таких как удостоверение, роль, разрешения, права и т.д. Авторизация на основании утверждений обеспечивает дополнительные уровни абстракции, упрощает отделение правил авторизации от механизма авторизации и аутентификации. Например, пользователь может быть подлинности по сертификату или имени пользователя / паролю, после чего набор этих утверждений передается в сервис для определения прав доступа к ресурсу.

Правильный выбор механизма управления *конфигурацией* имеет большое значение с точки зрения обеспечения безопасности и надежности программы, в противном случае, она будет уязвимой для различных атак. Также неправильный механизм управления конфигурацией может обусловливать расходы на администрирование. При проектировании стратегии управления конфигурацией руководствуйтесь такими рекомендациями:

– Тщательно продумывайте, какие параметры должны быть сконфигурированы извне. Убедитесь в реальной прикладной целесообразности каждого настраиваемого параметра и обеспечьте минимум параметров конфигурации, необходимый для выполнения этих требований.

– Примите решение о том, будут ли сведения о конфигурации храниться централизованно и загружаться или применяться к пользователям при запуске (например, через Active Directory Group Policy1). Продумайте, как обеспечит ограничение доступа к сведениям о конфигурации. Используйте меньше привилегированный процесс и учетные записи сервиса и приводить в конфиденциальные данные в хранилище конфигурации.

– Распределите элементы конфигурации по логическим разделам на основании того, они настройками пользователя, приложения или среды. Это упростит разделение конфигурации, если потребуется поддерживать различные настройки для различных наборов пользователей или множества сред.

– При наличии множества уровней в приложении распределите элементы конфигурации по логическим разделам. Если сервер приложений выполняется на веб-ферме, определите, какая часть конфигурации является общей, и какая часть применяется исключительно к компьютеру, на котором выполняется приложение.

– Предоставьте отдельный административный интерфейс пользователей для редактирования конфигурационных данных.

Проектирование эффективной стратегии управления исключениями имеет большое значение с точки зрения обеспечения безопасности и надежности программы. Неправильный выбор стратегии очень усложнит диагностику и решение проблем приложения, сделает его уязвимым для атак типа отказ в обслуживании (DoS), а также может привести к разглашению конфиденциальных и важных сведений. Формирование и обработка исключений является ресурсоемким процессом, поэтому важно, чтобы при проектировании были также учтены вопросы производительности. Хорошим подходом является проектирование централизованного механизма управления исключениями для программы и предоставление точек доступа к системе управления исключениями (как события WMI) для обеспечения поддержки систем мониторинга уровня предприятия, таких как Microsoft System Center. При проектировании стратегии управления *исключениями* руководствуйтесь такими рекомендациями:

– Проектируйте соответствующую стратегию распространения исключений, которая

обеспечивает обертывания или замену исключений или внесения необходимых сведений. Применяйте контекстные идентификаторы, это позволит находить взаимосвязанные исключения в разных слоях при проведении анализа главных причин погрешностей и сбоев. Перехватывайте внутренние исключения, только если можете обработать или должны добавить некоторые данные. Не использует исключения для управления логикой приложения.

– Обеспечьте, чтобы приложение не оставался в нестабильном состоянии после сбоя, и чтобы исключения не приводили к разглашению конфиденциальных данных или сведений о процессе. Если не можете гарантированно обеспечить корректное восстановление после сбоя, позвольте приложении завершиться с необработанным исключением; это лучше, чем оно будет продолжать выполнение в неизвестном и, возможно, поврежденном состоянии.

– Выработайте соответствующую стратегию протоколирования и уведомления для критических ошибок и исключений, обеспечивая сохранение достаточно детальных сведений об исключении. Это позволит техническому персоналу восстановить сценарий, который привел к исключению. Однако не предоставляйте конфиденциальные данные в сообщениях об исключении и файлы журнала.

– Проектирование эффективной стратегии протоколирования и инструментирования имеет большое значение с точки зрения обеспечения безопасности и надежности приложения, иначе пользователи смогут безнаказанно отказываться от своих действий. Также файлы журналов могут использоваться для доказательства правонарушений в случае судебного разбирательства. Аудит и протоколирование действий во всех слоях приложения нужны, так как могут помочь обнаружить подозрительные действия и обеспечить раннее выявление компьютерных атак.

При проектировании стратегии *протоколирования* и инструментовки руководствуйтесь такими рекомендациями:

– Проектируйте централизованный механизм протоколирования и инструментовки, что обеспечивает перехват критически важных для системы и бизнеса событий. Избегайте слишком детализированного протоколирования и инструментовки, но предусмотрите дополнительные функции протоколирования и инструментовки, настраиваемые во время выполнения, для получения дополнительных данных и для помощи при отладке.

– Создавайте политики безопасного управления файлами журнала. Не держите конфиденциальные данные в файлах журнала и защищайте от несанкционированного доступа. Продумайте, как обеспечить безопасный доступ и передачу данных аудита и протоколирования между слоями приложения, и обеспечьте сдерживание и правильную обработку сбоев протоколирования.

– Сделайте свои приемники журнала, или слушатели трассировки, настраиваемые, чтобы обеспечить возможность их изменения во время выполнения в соответствии с требованиями инфраструктуры развертывания. В реализации протоколирования и инструментовки в приложении очень помогут такие библиотеки, как Enterprise Library группы patterns & practices. Среди популярных библиотек можно вспомнить NLog илog4net.

Управление состоянием – это вопросы, связанные с хранением данных, приводят состояние компонента, операции или этапа процесса. Для хранения данных состояния могут использоваться различные форматы и хранилища. Механизм управления состоянием может оказывать влияние на производительность приложения; сохранения даже небольших объемов данных состояния может неблагоприятно сказываться на производительности приложения и его способности масштабироваться. При проектировании стратегии *управления состоянием* руководствуйтесь такими рекомендациями:

– Храните минимальный объем данных состояния. Если для сохранения или совместного использования эти состояния должны передаваться через границы процессов и сетей, обеспечьте их сериализуемость.

– Правильно выбирайте хранилище состояния. Хранение состояния в процессе или в памяти обеспечит лучшую производительность, но эта техника может использоваться, только если состояние не должен храниться между повторными запусками процесса или системы. Если

хотите, чтобы эти состояния были доступны после перезапуска процесса или системы, храните их на локальном диске или локальном SQL Server. Если состояние является критически важным аспектом приложения, или если эти состояния должны использоваться совместно несколькими компьютерами, храните состояние централизованного, например, на выделенном SQL Server.

Выводы

Разработаны методические рекомендации по использованию методов и средств распределения доступа и защиты данных в КИУС критического применения.

Разработана имитационная модель системы распределения доступа и защиты информации в КИУС критического применения, которая позволила провести экспериментальные исследования и оценить эффективность использования разработанных моделей и методов в системе обеспечения безопасности информации. Результаты экспериментов показали, что использование предложенных моделей и методов позволит в 1,5 раза увеличить время безопасного функционирования системы.

Список использованной литературы

1. Семенов С. Г. Методы и средства распределения доступа и защиты данных в компьютеризированных информационных управляющих системах критического применения/ С. Г. Семенов. – Х.:НТУ «ХПИ», 2013. – 360 с. Режим доступу: URL: http://www.docme.ru/doc/6625/rukovodstvo-microsoft®-po-proektirovaniyu-arhitektury-pril

2. Можаев А. А. Анализ и модели самоподобного трафика. Авиационно-космическая техника и технология./ А. А.Можаев, Г. А. Кучук, А. В. Воробьёв– 2006. –№ 9 (35). – С. 173–180.

3. Семенов С. Г. Анализ и синтез защищенных компьютерных систем и сетей / С. Г. Семенов, А. А. Подорожняк, А. И. Баленко // Х:НТУ«ХПИ», - 2012.

4. Семенов С. Г. Модели и методы управления сетевыми ресурсами в информационно-телекоммуникационных системах / С. Г. Семенов, А. А. Смирнов, Е. В. Мелешко // Х.:НТУ«ХПИ», 2012.

5. Можаев А. А. Усовершенствование математической модели защищенной информационно-телекоммуникационной системы с использованием теории чувствительности. / Семенов С. Г., Можаев М. А., Казимирова В. В. //– Киев. - Киев НТУУ КПИ. – 2013. – С. 167.

6. Семенов С. Г. Структурно-информационный портрет информационной системы в условиях неопределенности на примере Dos-атаки / С. Г. Семенов // Всеукраинский межведомственный научно-технический сборник «Радиотехника» Тематичний випуск: Информационная безопасность, - Х.: ХНУРЕ, – 2011 .– №166 .– С. 99–106.

7. Семенов С. Г. Методика математического моделирования защищенной ИТС на основе многослойной GERT-сети / С. Г. Семенов // Вісник Національного технічного університету «Харківський політехнічний інститут». Зб. наукових праць. Тематичний випуск: Інформатика і моделювання. – Х.: НТУ «ХПІ». – 2012. –№ 62 (968). – С 173–181.

8. Семенов С. Г. Оптимальное распределение канальных ресурсов в статистическом мультиплексоре по критерию минимального сбалансированного времени доставки информационных пакетов / С. Г. Семенов // мат. IV НТК ХУ ПС. – Х: ХУ ПС – 2008 – С. 151.

9. Semenov S. G. The method of processing and identification of telecommunication traffic based on BDS-tests / S. G. Semenov, O. A. Smirnov, E. V. Meleshko // The book of materials International Conference «Statistical Methods of Signal and Data Processing (SMSDP-2010)». – Kiev, Ukraine, National Aviation University “NAU-Druk” Publishing House, October 2010. – P. 166–168.

10. GetSystemTimes function [Електронний ресурс]. – Режим доступу до ресурсу: http://msdn.microsoft.com/en-us/library/windows/desktop/ ms724400(v=vs.85).aspx

References

1. .Semenov S. G. Methods and means of access and distribution of data protection in computerized information management systems, critical application / S.G. Semenov. – H.: NTU "KPI", 2013 – 360 p. Mode of access: URL: http://www.docme.ru/doc/6625/rukovodstvo-microsoft®-po-proektirovaniyu-arhitektury-pril

2.Mozhaev A. A. Analysis and models of self-similar traffic. Aerospace equipment and technology / A. A. Mozhaev, G. A. Kucuk, AV Vorobëv – 2006 - Number 9 (35). – S. 173–180.

3.Semenov S. G. Analysis and synthesis of the protected computer systems and networks / S. G. Semenov, A. A. Podorozhnyak, A. I. Balenko // X: NTU "KPI", – 2012.

4.Semenov S. G. Models and methods for managing network resources in information and telecommunication systems / S. G. Semenov, A. A. Smirnov, E.V. Myaleshka // H.: NTU "KPI", 2012.

5.Mozhaev A. A. Improvement of mathematical model of the protected information and telecommunication system using the theory of sensitivity. / S. G .Semenov, M. A. Mozhaev , V. V. Kazimirova // – Kiev. – Kiev NTU KPI. – 2013 – P. 167.

6. Semenov S. G. Structurally informative portrait of an information system in the face of uncertainty on the example of Dos-attack / S. G Semenov // Ukrainian interdepartmental scientific and technical collection "Radio"

tematichnee Preview Issue: Information Security – H.: KhNURE, – 2011. – № 166 . – P. 99–106.

7. Semenov S. G. Mathematical modeling technique protected ITS based on a multilayer GERT-network / SG Semenov // News Natsionalnogo tehnichnogo universitetu "Harkivsky politehnichny institut." SC. Naukova Pratzen. Tematichnee Preview Issue: Informatika i modelyuvannya. – H.: NTU "KhPI." – 2012. – № 62 (968). – P. 173–181.

8. Semenov S .G. Optimal allocation of channel resources in a statistical multiplexer by the criterion of the minimum balance-time delivery of information packets / S.G. Semenov // mat. IV STC HU PS. – X: XY PS – 2008 – P. 151.

9. Semenov S. G. The method of processing and identification of telecommunication traffic based on BDS-tests / S. G. Semenov, O. A. Smirnov, E.V. Meleshko // The book of materials International Conference «Statistical Methods of Signal and Data Processing (SMSDP-2010)." – Kiev, Ukraine, National Aviation University "NAU-Druk" Publishing House, October 2010. – P. 166–168.

10. GetSystemTimes function [E-resource]. - Mode of access to the resource: http://msdn.microsoft.com/en-us/library/windows/desktop/ ms724400 (v = vs.85) .aspx

Поступила в редакцию 20.07 2014 г.